REMARKS

Claims 2, 6, 7, 27, and 28 are canceled. Claims 1, 20-22, 24, 29, 32, and 38-40 are amended. Claims 1, 3-5, 8-27 and 29-41 remain in the Application. Reconsideration of the pending claims is respectfully requested in view of the above amendments and the following remarks.

The above claim amendments merely include subject matter in canceled claims. No new matter is added and no new issue is raised by the amendments. Thus, entry of the above amendments is respectfully requested.

I. Claims Rejected Under 35 U.S.C. § 103

A. Claims 1-5, 12, 13, 17-22, 24, 26, and 34-40 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,953,424 issued to Vogelesang et al. ("Vogelesang"), in view of Menezes, Alfred J., Handbook of Applied Crytography, CRC Press, 1997, pages 234-237 ("Menezes").

To establish a *prima facie* case of obviousness, the relied upon references must teach or suggest every limitation of the claim such that the invention as a whole would have been obvious at the time the invention was made to one skilled in the art.

Claim 1 is amended to include all of the limitations of canceled Claims 6 and 7. Among other elements, amended Claim 1 recites

> "generating, at the first entity, a first secret S_B using a combining function f_B on at least a first password P_B, the first public key M_B, and the second public key M_A;
>
> generating, at the first entity, a first session key K_B, the first session key K_B being different from the first secret S_B, both the first session key K_B and the first secret S_B being computed from the second public key M_A;
>
> encrypting, at the first entity, a first random nonce N_B with the first session key K_B or the first secret S_B to obtain a first encrypted result;
>
> encrypting, at the first entity, the first encrypted result with the other one of the first session key K_B or the first secret S_B to obtain an encrypted random nonce" (emphasis added).

Applicants submit that Vogelesang in view of Menezes does not teach or suggest at least these elements.

Vogelesang discloses a cryptographic system in which signals between two participants are encrypted with one encryption key (i.e., a shared secret S). The Examiner recognizes that Vogelesang does not disclose encryption with two encryption keys, but relies on Menezes to cure this deficiency. Menezes discloses encrypting a message with two encryption keys. However, Menezes does not teach or suggest using the first session key K_B and the first secret S_B as the two encryption keys, where S_B is computed using a combining function f_B on at least a first password P_B, the first public key M_B, and the second public key M_A. Thus, Vogelesang is view of Menezes does not teach or suggest each of the elements of amended Claim 1.

Further, Claim 1 is amended to incorporate all of the limitations of canceled Claims 6 and 7. In the Final Office Action, Claims 6 and 7 are rejected over Vogelesang in view of Menezes and further in view of Wu, Thomas, "The Secure Remote Password Protocol," November 11, 1997, Stanford University, pages 1-17 ("Wu").

Wu does not cure the deficiencies of Vogelesang and Menezes. Wu is relied on for disclosing the use of a combining function f_B that combines at least a first password P_B and the first public key M_B to generate the first secret S_B. Wu discloses an equation for generating a public key $B = v + g^b$, and another equation for generating a secret $S = (B - g^x)^(a + ux)$ (see Table 4). Wu further discloses that the variable x is derived from a user's password P. Thus, the secret S is characterized as a combination of at least the password P and the public key B. However, the secret S is not used as an encryption key. Rather, the secret S is hashed and transmitted to the other party without encryptions (see Table 4). Thus, even assuming, for the sake of argument, that Wu discloses using a combining function to generate a secret, the secret disclosed by Wu is not an encryption key. Thus, the disclosure of Wu does not teach or suggest the claimed first secret S_B, which encrypts the first random nonce N_B.

Moreover, there is no motivation to combine Wu with Vogelesang and Menezes, because Wu specifically discloses that the algorithm involves no encryption. Under the section heading "Asymmetric Key Exchange" (AKE), Wu discloses the following:

> "Like EKE, the primary function of AKE is to exchange keys between two parties, the client and server, and to use this key to verify that both parties actually know their passwords. Unlike EKE, AKE does not encrypt any of the protocol flows. Instead, it uses predefined mathematical relationships to combine exchanged ephemeral values

with established password parameters. Avoiding encryption is advantageous for a number of reasons...." (emphasis added).

Wu teaches that encryption should be avoided. Thus, Wu has specifically taught away from combining the AKE algorithm with the encryption algorithms of Vogelesang and Menezes. See MPEP § 2143.01. The Prior Art Must Suggest the Desirability of the Claimed Invention. Thus, the Examiner's proposed combination is inapposite.

Claims 2-5, 12, 13, and 17-19 depend from Claim 1 and incorporate the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claim 1, these claims are non-obvious over the cited references. Analogous discussions apply to independent Claims 20-22, 24, and 38-40, which are amended to include similar limitations. Claims 26 and 34-37 depend from Claim 24 and incorporate the limitations thereof. Thus, for at least the reasons mentioned above, these claims are non-obvious over the cited references.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claims 1-5, 12, 13, 17-22, 24, 26, and 34-40 are respectfully requested.

B. Claims 6-9, 11, and 27-32 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Vogelesang in view of Menezes in further view of Wu, Thomas, "The Secure Remote Password Protocol," November 11, 1997, Stanford University, pages 1-17 ("Wu").

Claims 6, 7, 27, and 28 are canceled. Claims 8, 9, 11, and 29-32 depend from Claims 1 and 24, respectively, and incorporate the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claims 1 and 24, Vogelesang in view of Menezes and further in view of Wu does not teach or suggest each of the elements of these claims.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claims 6-9, 11, and 27-32 are respectfully requested.

C. Claims 10 and 31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Vogelesang in view of Menezes, and further in view of Wu.

Claims 10 and 31 depend from Claims 1 and 24, respectively, and incorporate the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claims 1 and 24, the cited references do not teach or suggest each element of these claims.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claims 10 and 31 are respectfully requested.

D. Claims 14-16, 25, and 33 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Vogelesang in view of Menezes.

Claims 14-16, 25, and 33 depend from Claims 1 and 24, respectively, and incorporate the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claims 1 and 24, Vogelesang in view of Menezes does not teach or suggest each of the elements of these dependent claims.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claims 14-16, 25 and 33 are requested.

E. Claim 41 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Vogelesang in view of Menezes.

Claim 41 depends from Claim 40 and incorporates the limitations thereof. Claim 40 is non-obvious over the cited references for reasons analogous to Claim 1. Thus, for at least the reasons mentioned above in regard to Claim 1, the cited references do not teach or suggest each of the elements of Claim 40 and its dependent claim, namely, Claim 41.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claim 41 are requested.

F. Claim 23 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Vogelesang in view of Menezes.

Claim 23 depends from Claim 1 and incorporates the limitations thereof. Thus, for at least the reasons mentioned above in regard to Claim 1, the cited references do not teach or suggest each of the elements of Claim 23.

Accordingly, reconsideration and withdrawal of the § 103 rejection of Claim 23 are requested.

CONCLUSION

In view of the foregoing, it is believed that all claims are now in condition for allowance and such action is earnestly solicited at the earliest possible date. If there are any additional fees due in connection with the filing of this response, please charge those fees to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: January 18, 2007

Jonathan S. Miller, Reg. No. 48,534

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
Telephone (310) 207-3800
Facsimile (310) 820-5988

CERTIFICATE OF FACSIMILE

I hereby certify that this correspondence is being transmitted via facsimile on the date shown below to the United States Patent and Trademark Office.

Amber D. Saunders 1/18/2007

Amber D. Saunders Date